Mamoru South Africa (Pty) Ltd

IT Security Policy
Version 1.0

Table of Contents

1. Introduction

This policy documents the IT Security management and mitigation of Mamoru South Africa (Pty) Ltd (Mamoru or the “Company”). It is the primary responsibility of the Company to ensure that the risks pertaining to the business are effectively managed. The Company will seek to understand its exposure to IT risks and is putting in place a robust risk management framework to ensure IT and cyber resilience. The IT Security Policy and measures developed by the Company commensurate its business model and the Company will review them periodically whenever it reviews its business model, operational model or products and services offered to its customers.

2. Scope

The IT Security Policy and its supporting controls, processes and procedures apply to all IT infrastructure used at Mamoru to ensure safety level in Hardware, Software, access rules and passwords rules.

3. Role and responsibilities

The Board of Directors (”BoD”) and Senior Management should exercise effective oversight of the risk management processes undertaken by relevant functions, especially the IT security function. The Board of Directors and Senior Management will ensure that this key function is implemented efficiently following all recommendations and reporting of the IT Management team. All Mamoru’s employees must comply with the processes outlined in this document.

The Board of Directors is responsible for:

a) ensuring a sound and robust risk management framework is established and maintained to manage IT risks;
b) ensuring there is an IT risk management function to oversee the IT risk management framework and strategy, as well as to provide an independent view of the IT risks faced by the Company;
c) approving the risk appetite and risk tolerance statement that articulates the nature and extent of IT risks that the Company is willing and able to assume;
d) undertaking regular reviews of the IT risk management strategy for continued relevance;
e) assessing management competencies for managing IT risks; and
f) ensuring an audit function is established to assess the effectiveness of controls, risk management and governance of the Company.

Senior management of the Company is responsible for:

a) establishing the IT risk management framework and strategy;
b) managing IT risks based on the established framework and strategy;
c) ensuring sound and prudent policies, standards and procedures for managing IT risks are established and maintained, and that standards and procedures are implemented effectively;

d) ensuring the roles and responsibilities of staff in managing IT risks are delineated clearly; and
e) apprising the Board of Directors of salient and adverse IT risk developments and incidents that are likely to have a major impact on the Company in a timely manner.

Compliance with the controls in this policy will be monitored by the Information Security Team and reported to the BoD.

4. IT Risk Management Framework

The Company will establish a risk management framework to manage its IT risks.

The risk management framework will encompass the following components:

- risk identification: the Company will identify threats and vulnerabilities to the Company and information assets;

- risk assessment: the Company will assess the potential impact and likelihood of threats and vulnerabilities to the Company and information assets;

- risk treatment: the Company will develop and implement processes and controls to manage IT risks posed to the Company and protect the confidentiality, integrity and availability of information assets; and

- risk monitoring, review and reporting: the Company will monitor and review IT risks, which include risks that customers are exposed to, changes in business strategy, IT systems, environmental or operating conditions, and report key risks to the BoD and Senior Management.

5. IT Threats and vulnerabilities

A vulnerability is a weakness in a system, system security procedure, internal controls, or implementation that could be exploited by a threat source. Vulnerabilities leave systems susceptible to a multitude of activities that can result in significant and sometimes irreversible losses to an individual, group, or organisation. These losses can range from a single damaged file on a laptop computer or mobile device to entire databases at an operations centre being compromised. With the right tools and knowledge, an adversary can exploit system vulnerabilities and gain access to the information stored on them. The damage inflicted on compromised systems can vary depending on the threat source.

In order to protect a system from risk and to implement the most cost-effective security measures, the Company will ensure that system owners, managers, and users know and understand the vulnerabilities of the system as well as the threat sources and events that may exploit the vulnerabilities. When determining the appropriate response to a discovered vulnerability, care should be taken to minimise the expenditure of resources on vulnerabilities where little or no threat is present.

The Company shall monitor and prevent the risk arising out of the following threats and vulnerabilities:

a) Fraud and theft: Systems can be exploited for fraud and theft by "automating" traditional methods of fraud or by utilising new methods. System fraud and theft can be committed by insiders (i.e. authorised users) and outsiders. Authorised system administrators and users with access to and familiarity with the system (e.g., resources it controls, flaws) are often responsible for fraud.
b) Malicious hacker attacks: Malicious hacker is a term used to describe an individual or group who use an understanding of systems, networking, and programming to illegally access systems, cause damage, or steal information. The Company shall understand the motivation that drives a malicious hacker in order to implement the proper security controls to prevent the likelihood of a system breach.
c) Malicious code: Malicious code refers to viruses, Trojan horses, worms, logic bombs, and any other software created for the purpose of attacking a platform. The Company will closely monitor its IT systems and require its employees to report any virus threats. If necessary, the affected areas will be shut down in order to stop the virus from penetration in other systems.

6. IT Systems reliability, availability and recoverability

6.1. System availability

Maintaining system availability is crucial in achieving confidence and trust in the Mamoru's operational capabilities. IT systems should be designed and implemented to achieve the level of system availability that is commensurate with its business needs. The Company will seek to achieve high availability for crucial systems. The Company will develop the built-in redundancies to reduce single points of failure which can bring the entire network down.

The Company will ensure system availability by minimising disruption to the normal business activities that the Company engages in. All changes (including IT systems provided by third party service providers) must follow the change management process. The key processes include:

a) All changes must be logged in the system
b) Changes should be assessed by the Head of Information Technology and they should be in line with the operational needs
c) Appropriate level of testing should be undertaken prior to the formal implementation and the testing results should be fully approved by the Head of Information Technology (or the Executive Director in case of emergency)
d) All security testing activities should be performed in a non-production environment
e) If changes are deemed to present unacceptable level of risks during the Head of information Technology's assessment, such changes should be denied and documented.
f) As a general principle, implementation of changes should be carried out outside of normal trading hours unless emergency. Stakeholders (e.g. traders, operations, clients) should be notified immediately in the case of emergency.

6.2. System recoverability

The Company will develop a disaster recovery plan and will include a scenario analysis to identify and address various types of contingency scenarios.
The following scenarios will be considered: (a) major system outages; (b) hardware malfunction; (c) operating errors or security incidents etc.

The Company will define system recovery and business resumption priorities based on its IT systems in operation at each point of the Company's development. The recovery time objective for the for each of the critical systems should not be more than 4 hours within any period of 12 months.
The recovery point objective will be established for each critical system based on the system's characteristics and Company's reliability of this system.
The Company will perform a disaster recovery testing of its systems in order to test the effectiveness of its disaster recovery plans. During disaster recovery testing the Company will cover various scenarios, including total shutdown or incapacitation of the primary site as well as component failure at the individual system or application cluster level.
If employees cannot access business premises due to natural disasters or other emergencies, they will be able to remotely connect to any one of the Company servers from any computer with an internet connection. Offsite server will be accessible via SSL VPN connection.

6.3. System backup and recovery

The Company will establish a system and data backup strategy and develop a plan to perform regular backups so that systems and data can be recovered in the event of a system disruption or when data is corrupted or deleted.
To ensure data availability is aligned with the Company's business requirements, the Company will develop a policy to manage the backup data life cycle, which includes the establishment of the frequency of data backup and data retention period, management of data storage mechanisms, and secure destruction of backup data.
The Company will ensure that any confidential or sensitive information is stored in the backup media securely such as through the encryption of such data.
Data are regularly backed up to a secure location such that all data are fully recoverable promptly in the event of a hardware failure. This is achieved mainly through differential backups (incremental backups on weekday and full backups on weekend). The Company maintains at least two backup versions of its critical data and information. At a minimum, one fully recoverable version of the backup is stored in a secure offsite location. The Company periodically tests the backup data and trial restoration.

7. Access Control

7.1. User Access Management

The Company will follow the principles known as “never alone”, “segregation of duties” and “least privilege” when granting staff access to information assets so that no one person has access to perform sensitive system functions.
Access rights and system privileges will be granted according to the roles and responsibilities of the staff, contractors and service providers.
Mamoru will establish a user access management process to provision, change and revoke access rights to information assets. Access rights should be authorised and approved by appropriate parties, such as the information asset owner.

Multi-factor authentication(“MFA”) will be implemented for the following:
(a) all administrative accounts in respect of any operating system, database, application, security appliance or network device that is a critical system; and
(b) all accounts on any system used by the relevant entity to access customer information through the internet.

7.2. Privileged Access Management

Users will only be granted access rights on a need-to-use basis. Access rights that are no longer needed, as a result of a change in a user’s job responsibilities or employment status (e.g. transfer or termination of employment), should be revoked or disabled promptly.

The Company will closely supervise staff with elevated system access entitlements and have all their systems activities logged and reviewed as they have the knowledge and resources to circumvent systems controls and security procedures. The Company will adopt the following controls and security practices:

a) Implement strong authentication mechanisms such as two-factor authentication for privileged users;
b) Institute strong controls over remote access by privileged users;
c) Restrict the number of privileged users;
d) Grant privileged access on a “need-to-have” basis;
e) Maintain audit logging of system activities performed by privileged users;
f) Disallow privileged users from accessing systems logs in which their activities are being captured;
g) Review privileged users’ activities on a timely basis;
h) Prohibit sharing of privileged accounts;
i) Disallow vendors and contractors from gaining privileged access to systems without close supervision and monitoring; and
j) Protect backup data from unauthorised access.

The Company will subject its service providers, who are given access to the Company’s information assets, to the same monitoring and access restrictions on the Company’s staff.

In situations where the users are given a remote access control the Company will ensure that it is only allowed from the devices that have been secured according to the Company's security standards.
The access control is normally reviewed upon triggering events such as new joining, staff departure, material changes in business operations and internal re-assignment of employee duties.

8. Information Security Policies

8.1. Data Security

The Company will develop comprehensive data loss prevention policies and adopt measures to detect and prevent unauthorised access, modification, copying, or transmission of its confidential data, taking into consideration the following:

a) data in motion: data that traverses a network or that is transported between sites;
b) data at rest: data in endpoint devices such as notebooks, personal computers, portable storage devices and mobile devices, as well as data in systems such as files stored on servers, databases, backup media and storage platforms (e.g. cloud); and
c) data in use: data that is being used or processed by a system.

The Company will implement appropriate measures to prevent and detect data theft, as well as unauthorised modification in systems and endpoint devices. Mamoru will ensure systems managed by its service providers are accorded the same level of protection and subject to the same security standards.
Systems and endpoint devices are often targeted by cyber criminals to gain access or exfiltrate confidential data within an organisation. As such, confidential data stored in systems and endpoint devices should be encrypted and protected by strong access controls.
The Company will ensure only authorised data storage media, systems and endpoint devices are used to communicate, transfer, or store confidential data.
The Company has installed anti-virus and anti-malware software ("AV-AM") on Company computers. The AV-AM software is managed by IT staff who checks and updates all AV-AM definitions daily.
The AV-AM software performs regular scheduled scans and unscheduled scans manually triggered when necessary.
Whenever a new or updated AV-AM software is feasible available and is of minimal impact to the users, prompt implementation will be arranged.

8.2. Basic Principles of Information Security

Each employee, counterparty and business partner having access to information must comply with below basic information security principles:

- Clean desk policy: when leaving your workstation, you must not leave any documents on the desk as well as other data carriers containing all important

information, in particular customers personal data. All documents and data carriers containing information other than public should be stored in lockable storage cabinets. After finishing work, the documents should be cleared from the desk.

- Clear screen policy: each time you leave your workstation even for a moment, remember to block access to the computer. It protects your computer from unauthorised access to confidential information.
- Use confidential waste bins and shredders: use a shredder or a confidential waste bin to destroy all official documents. Under no circumstances must you dispose of your business documents in a trash can. Issues such as identity theft mean that you should never assume that because a document has been put in the bin, it will not be viewed by anyone else. It is essential to protect both electronic and printed data and to do so please use shredders available on every floor.
- Hardware protection: do not leave unattended Company's equipment or other media containing business information. It is essential to look after laptops that are carried outside the Company's premises and do not leave them alone, i.e. in cars.
- Secure printing: pick up documents from the printers as soon as they are printed - documents cannot be stored on the printers. It is recommended to use the "Secure Print" function, which allows you to secure the print with a PIN code. The document will not be printed until you enter the code on the printer. This solution is especially recommended in situations where the printer is in a different room, for example in the corridor.
- Secure information in mails: secure in an appropriate manner all attachments and files containing confidential information, i.e. encrypt or protect by password. It is not allowed to include confidential information in the content of the email.
- Discreet conversations: you should avoid discussing confidential topics about the Company or its clients in public places or even in the third parties. It should be remembered that during conversations in public places it is not allowed to mention the names of people and details of matters that would allow to easy identification.

8.3. Network Security Principles

The Company will install network security devices such as firewalls to secure the network between the Mamoru and the Internet, as well as connections with third parties.
To minimise the risk of cyber threats, such as lateral movement and insider threat, the Company will deploy effective security mechanisms to protect information assets. Information assets could be grouped into network segments based on the criticality of systems, the system's functional role (e.g. database and application) or the sensitivity of the data.
Network intrusion prevention systems should be deployed in the Company's network to detect and block malicious network traffic.
The Company will implement network access controls to detect and prevent unauthorised devices from connecting to its network.

Network access control rules in network devices such as firewalls, routers, switches and access points should be reviewed on a regular basis to ensure they are kept up-to-date. Obsolete rules and insecure network protocols should be removed promptly as these can be exploited to gain unauthorised access to the Company's network and systems.
Internet web browsing provides a conduit for cyber criminals to access the Company's IT systems. In this regard, the Company will consider isolating internet web browsing activities from its endpoint devices using physical or logical controls, or implement equivalent controls, to reduce exposure of its IT systems to cyber-attacks.
The Company will periodically review its network security design, network interconnections and potential cyber security vulnerabilities.

8.4. System Security

The security standards for Mamoru's hardware and software (e.g. operating systems, databases, network devices and endpoint devices) should outline the configurations that will minimise their exposure to cyber threats. The standards should be reviewed periodically for relevance and effectiveness.
The Company will establish a process to verify that the standards are applied uniformly on systems and to identify deviations from the standards. Risks arising from deviations should be addressed in a timely manner.
Endpoint protection, which includes but is not limited to behavioural-based and signature-based solutions, should be implemented to protect the Company from malware infection and address common delivery channels of malware, such as malicious links, websites, email attachments or infected removable storage media.
The Company will ensure that anti-malware signatures are kept updated, and the systems are regularly scanned for malicious files or anomalous activities.
To facilitate early detection and prompt remediation of suspicious or malicious systems activities, Mamoru implement detection and response mechanisms to perform scanning of indicators of compromise ("IOCs") in a timely manner, and proactively monitor systems', including endpoint systems', processes for anomalies and suspicious activities.

9. Notification to the Financial Sector Conduct Authority

The Company shall notify without delay the Financial Sector Conduct Authority("FSCA"), when the Company becomes aware of a major operational or security incident.

10. Information Security Audit

The Company should ensure that the scope of IT audit is comprehensive and includes all critical IT operations.

A comprehensive set of auditable areas for IT risk should be identified so that an effective risk assessment could be performed during internal and external audit

planning to demonstrate compliance with regulations, standards and best practice. Auditable areas are identified to include all IT operations, functions and processes.
The Company will conduct IT audit on a periodical basis and the frequency will be defined by the criticality of and risk posed by its IT information assets, functions and processes.
Mamoru will ensure its IT auditors have the requisite level of competency and skills to effectively assess and evaluate the adequacy of IT policies, procedures, processes and controls implemented.